

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1170	kocher.inv.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:30
L2	15	"380"/\$.ccls. and kocher.inv.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:33
L3	104	"380"/\$.ccls. and darrow.xp.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:33
L6	15	I3 and ((elliptic\$3 near curve) "ECC")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:35
L8	288	((elliptical\$3 near curve) or "Koblitz curve" "ECC") with ((public near key) (crypto\$5 near algorithm))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:40
L9	10	I8 and ("DPA" or "differential power analysis" or "power analysis attacks")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:38
L10	70	380/28-30.ccls. and ("DPA" or "differential power analysis" or "power analysis attacks")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:39
L12	9	380/28-30.ccls. and (select\$3 determin\$3 draw\$3 calculat\$3 computing) near3 (security adj (parameter value variable))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:41
L13	15	708/490-492.ccls. and ((elliptical\$3 near curve) or "Koblitz curve" "ECC") with ((public near key) (crypto\$5 near algorithm))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:41
L14	87	380/28-30.ccls. and ((scalar adj multipl\$7) and (elliptic\$4 adj curve))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:43

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1170	kocher.inv.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:30
L2	15	"380"/\$.ccls. and kocher.inv.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:33
L3	104	"380"/\$.ccls. and darrow.xp.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:33
L6	15	l3 and ((elliptic\$3 near curve) "ECC")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:35
L8	288	((elliptical\$3 near curve) or "Koblitz curve" "ECC") with ((public near key) (crypto\$5 near algorithm))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:40
L9	10	l8 and ("DPA" or "differential power analysis" or "power analysis attacks")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:38
L10	70	380/28-30.ccls. and ("DPA" or "differential power analysis" or "power analysis attacks")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:39
L12	9	380/28-30.ccls. and (select\$3 determin\$3 draw\$3 calculat\$3 computing) near3 (security adj (parameter value variable))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 11:15
L13	15	708/490-492.ccls. and ((elliptical\$3 near curve) or "Koblitz curve" "ECC") with ((public near key) (crypto\$5 near algorithm))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:41
L14	87	380/28-30.ccls. and ((scalar adj multipl\$7) and (elliptic\$4 adj curve))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 10:43

EAST Search History

L15	53	((elliptic\$3 near curve) and (public near key) and (random near number)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 11:15
L17	5	((elliptic\$3 near curve) and (public near key) and (random near number) and (scalar)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 11:14
L18	31	((elliptic\$3 near curve) and (public near key) and (random near number) and (private near key)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/01 11:14



Web Images Video News Maps more »

Search Patents

Advanced Patent Search
Google Patent Search Help

Sign in

Lowercase "or" was ignored. Try "OR" to search for either of two terms. [\[details\]](#)

Patents

Patents 1 - 8 on ("DPA" or "differential power analysis" or "power analysis attacks"). (0.10 seconds)

System and method for preventing differential power analysis attacks (DPA) on a cryptographic device

US Pat. 6766455 - Filed Dec 9, 1999 - Pitney Bowes Inc.

... SYSTEM AND METHOD FOR PREVENTING DIFFERENTIAL POWER ANALYSIS ATTACKS (DPA) ON A CRYPTOGRAPHIC DEVICE RELATED APPLICATIONS The present application shares ...

Method of preventing power analysis attacks on microelectronic assemblies

US Pat. 6298135 - Filed Apr 29, 1999 - Motorola, Inc.

... BI METHOD OF PREVENTING POWER ANALYSIS ATTACKS ON MICROELECTRONIC ASSEMBLIES

... to more complex techniques, such as differential power analysis (DPA). ...

Method and apparatus for minimizing differential power attacks on processors

US Pat. 7092523 - Filed Jul 10, 2001 - Certicom Corp.

The DPA vulnerabilities result from transistor and the priority of Canadian Patent

... cessful power analysis attacks on processors. particularly on smart ...

Method for protecting an electronic system with modular exponentiation-based cryptography ...

US Pat. 6973190 - Filed Oct 26, 2000 - CP8 Technologies

CRYPTOGRAPHY AGAINST ATTACKS BY The so called high-order power analysis attacks are a PHYSICAL ANALYSIS 5 generalization of the DPA attack described above. ...

Space-efficient, side-channel attack resistant table lookups

US Pat. 7142670 - Filed Aug 31, 2001 - International Business Machines Corporation

... some examples being Timing attacks (TA), Simple Power Analysis attacks (SPA),

Differential Power Analysis attacks (DPA), Simple Electromagnetic Analysis ...

On-chip power supply interface with load-independent current demand

US Pat. 6963188 - Filed Apr 6, 2004 - Atmel Corporation

Differential power analysis (DPA) is a technique in which a chip's supply current is monitored externally for data- dependent variations that may indirectly ...

Countermeasure method in an electric component using a secret key cryptographic-algorithm

US Pat. 6820814 - Filed Jan 14, 2002 - Gegemplus

The basic idea of the **DPA** attack is thus to use the 7, 2000, ... with are referred to as **DPA (Differential Power Analysis) attacks**. a current consumption ...

System and method for suppressing conducted emissions by a cryptographic device comprising an ...

US Pat. 6748535 - Filed Dec 9, 1999 - Pitney Bowes Inc.

9, 1999; titled **SYSTEM AND METHOD FOR PREVENTING DIFFERENTIAL POWER ANALYSIS**

ATTACKS (DPA) ON A CRYPTOGRAPHIC DEVICE. BACKGROUND OF THE INVENTION 15 The ...

[Google Patent Search Help](#) | [Advanced Patent Search](#)

[Google Home](#) - [About Google](#) - [About Google Patent Search](#)

©2007 Google



Web Images Video News Maps [more »](#)

[Advanced Patent Search](#) [Google Patent Search Help](#)

[Sign in](#)

Patents

Patents **1 - 10** on **elliptic curve public key "random number" scalar**. (0.11 seconds)

Method and apparatus for elliptic curve cryptography and recording medium therefore

US Pat. 6876745 - Filed Dec 22, 1999 - Hitachi, Ltd.

Incidentally, it should be mentioned that the **elliptic curve** encryption ...

In a third step, the **public key Q** and the **random number k** generated in the first ...

Elliptic curve encryption method and system

US Pat. 6480606 - Filed Feb 23, 1999 - Hitachi, Ltd.

A **public/ private key** generating unit 102 generates a **public key 116** and a ...

The **elliptic curve** calculating unit 109 executes a **scalar multiplication** ...

Network system using a threshold secret sharing method

US Pat. 6477254 - Filed Feb 9, 1999 - Hitachi, Ltd.

50 Step 204: Using a **public key Q2** corresponding to the secret **key d2 108** and

the **random number k**, an operation is achieved on an **elliptic curve** to attain ...

Public-key-encryption data-communication system and data-communication-system forming method

US Pat. 6990583 - Filed Feb 26, 2001 - Sony Corporation

... on the **elliptic curve** by a **scalar** times, similarly to step S4 in FIG. 11. ...

When using a **public key** certificate, the user uses a **public 50 key** of the ...

Digital signature generating/verifying method and system using public key encryption

US Pat. 6341349 - Filed Oct 30, 1997 - Hitachi, Ltd.

PUBLIC KEY ENCRYPTION Step 2: A key QA is computed in accordance with **QA=dap**.

... to the process "**scalar multiplication on elliptic System Setup curve (E)**" ...

Public-key certificate issuance request processing system and public-key certificate issuance ...

US Pat. 7149894 - Filed Sep 13, 2001 - Sony Corporation

Herein, **Bk** denotes a **random number** and **Av public key** certificate. denotes a point

on the **curve** of the **elliptic** function. The FIG. 11 describes a sequence of ...

Public key certificate issuing system, public key certificate issuing method, information ...

US Pat. 7152158 - Filed Jan 9, 2002 - Sony Corporation

In step S15, "a" and "b" be coefficients of **elliptic curve** ($4a^3+27b^2 \neq 0$) 15 ...



Welcome United States Patent and Trademark Office

[Search Session History](#)[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Fri, 1 Jun 2007, 11:03:50 AM EST

Edit an existing query or
compose a new query in the
Search Query Display.

Search Query Display

Select a search number (#)
to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Recent Search Queries

- #1 ((differential power analysis<in>metadata) <or> (power analysis attack<in>metadata))
- #2 ((elliptic curve<in>metadata) <or> (elliptical curve<in>metadata))<or> (ecc<in>metadata)
- #3 (((differential power analysis<in>metadata) <or> (power analysis attack<in>metadata))) <AND> (((elliptic curve<in>metadata) <or> (elliptical curve<in>metadata)) <or> (ecc<in>metadata))
- #4 ((scalar multiplication<in>metadata) <or> (scalar multi<in>metadata))
- #5 (((elliptic curve<in>metadata) <or> (elliptical curve<in>metadata)) <or> (ecc<in>metadata)) <AND> (((scalar multiplication<in>metadata) <or> (scalar multi<in>metadata)))



Indexed by
 Inspec

[Help](#) [Contact Us](#) [Privacy &](#)

© Copyright 2006 IEEE -